

ANNEXE 7

Architecture et Sécurité
Nouvelle annexe

Intégrant l'addendum n°6 de Juillet 2010

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

Sommaire

1	INTRODUCTION	4
2	LES PERIPHERIQUES DU POSTE DE TRAVAIL	5
2.1	GENERALITES.....	5
2.2	ACCES AU RESEAU INTERNET.....	5
2.3	L'IMPRIMANTE.....	5
2.4	LE LECTEUR DE CODE A BARRES.....	5
2.5	LE LECTEUR SESAM-VITALE.....	6
3	LES ARCHITECTURES DU POSTE DE TRAVAIL	7
3.1	GENERALITES.....	7
3.2	DEFINITIONS	8
3.2.1	<i>Réseau local / Réseau distant</i>	8
3.2.2	<i>Exigences sécuritaires</i>	8
3.2.3	<i>Analyse sécuritaire</i>	8
3.3	L'ANALYSE SECURITAIRE DANS LE CADRE DE LA PROCEDURE D' AGREMENT.....	9
3.4	LES ARCHITECTURES « POSTE ISOLE » ET « RESEAU LOCAL ».....	10
3.4.1	<i>Généralités</i>	10
3.4.2	<i>Configuration 1 : Poste de travail mono-canal comportant un lecteur bi-fente homologué SESAM-Vitale</i>	10
3.4.3	<i>Configuration 2 : Poste de travail avec plusieurs canaux à gérer</i>	10
3.4.4	<i>Configuration 3 : Réseau local</i>	11
3.4.5	<i>Configuration 4 : Grappe de postes de travail en réseau local</i>	11
3.4.6	<i>Configuration 5 : Configurations « réseau local » mixtes</i>	12
3.5	LES EXIGENCES SECURITAIRES	13
3.5.1	<i>Avant-propos</i>	13
3.5.2	<i>Définitions</i>	13
3.5.3	<i>Références externes</i>	14
3.5.4	<i>Architecture des solutions</i>	15
3.5.5	<i>Les exigences de sécurité</i>	16
3.5.5.1	<i>Exigences générales</i>	16
3.5.5.2	<i>Exigences pour l'environnement local</i>	17
3.5.5.3	<i>Exigences sur les échanges via un réseau distant</i>	19
3.5.5.4	<i>Exigences pour l'environnement distant</i>	20
3.5.5.5	<i>Note</i>	21
3.6	LES ARCHITECTURES « RESEAU DISTANT »	22
3.6.1	<i>Configuration 6 : TLA(s) distant(s)</i>	22
3.6.2	<i>Configuration 7 : Gestion multiserveurs distants et multi postes de travail distants</i>	23
3.6.3	<i>Configurations 8 : Autres configurations</i>	24

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

1 INTRODUCTION

La présente annexe a pour but de décrire l'architecture technique du poste de travail du professionnel de santé ainsi que les différentes configurations techniques et sécuritaires autorisées dans le cadre de l'agrément SESAM-VITALE.

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

2 LES PERIPHERIQUES DU POSTE DE TRAVAIL

2.1 Généralités

Les composants suivants entrent en jeu dans l'élaboration et la transmission des factures électroniques nécessaires au remboursement des soins :

- l'équipement informatique : micro-ordinateur, unité centrale,
- un accès au réseau Internet (modem, ADSL, câble...),
- une imprimante (optionnelle),
- un lecteur de code à barres (optionnel),
- un dispositif de lecture de cartes à microprocesseur.

Ces éléments sont utilisables hors du contexte SESAM-Vitale.

2.2 Accès au réseau Internet

Afin d'effectuer la transmission des factures électroniques nécessaires au remboursement des soins, un accès :

- au réseau Internet (via modem, ADSL, câble...),
- ou à un réseau tiers permettant la transmission des factures électroniques soit vers Internet, soit vers le Réseau SESAM-Vitale,

doit être possible depuis l'équipement informatique du Professionnel de Santé.

En fonction de ses capacités, l'accès au réseau peut également être utilisé pour d'autres types de transfert de données (messagerie, télécopie, accès à des serveurs, etc.).

2.3 L'imprimante

L'imprimante est utilisable par tout progiciel existant sur l'équipement informatique du Professionnel de Santé : traitement de texte, gestion de cabinet, impression des ordonnances, impression des quittances remises aux assurés, etc.

Le présent document ne contient aucune spécification des périphériques d'impression.

2.4 Le lecteur de code à barres

Un lecteur de code à barres peut s'avérer utile pour faciliter la saisie des codes médicament présents sur les vignettes.

Un lecteur de code à barres peut également s'avérer utile pour faciliter la saisie des codes structure et RPPS éventuellement présents sur les ordonnances.

Le présent document ne contient aucune spécification relative aux périphériques de lecture de code à barres.

Réf. PDT-CDC-001	G.I.E. SESAM-VITALE	Page 5 / 24
------------------	---------------------	-------------

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

2.5 Le lecteur SESAM-Vitale

Le présent document ne contient aucune spécification du lecteur SESAM-Vitale. Le lecteur homologué SESAM-Vitale est un appareil programmable, répondant aux spécifications de l'Assurance Maladie qui participe à la sécurisation des transactions électroniques (homologué SESAM-Vitale).

Le lecteur SESAM-Vitale assure une compatibilité ascendante et descendante entre les différents types de cartes à microprocesseur.

Le logiciel lecteur SESAM-Vitale permet de lire toute carte compatible avec la norme ISO 7816 selon deux modes :

- le mode « transparent » dans lequel les données ne sont pas traitées,
- le mode « Intelligent » dans lequel les données sont traitées par une application implantée dans le lecteur (ex : filtre, interprétation, etc.).

Les caractéristiques techniques du lecteur SESAM-Vitale permettent, dans la limite de la capacité mémoire disponible, d'héberger plusieurs logiciels. Son système d'exploitation assure l'étanchéité entre les différents logiciels.

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

3 LES ARCHITECTURES DU POSTE DE TRAVAIL

3.1 Généralités

La configuration du poste de travail comprend au minimum un équipement informatique et un lecteur de facturation homologué SESAM-Vitale.

Le poste de travail du Professionnel de Santé intègre un ou plusieurs lecteurs SESAM-Vitale.

En ce qui concerne l'architecture des solutions présentées à l'agrément, celles-ci :

- soit sont limitées à un réseau local,
- soit font partie d'un réseau distant.

Le présent document présente diverses configurations techniques qui sont, à l'heure actuelle, acceptées dans le cadre de l'agrément SESAM Vitale.

Le présent document fournit également pour chacune de ces configurations les exigences techniques et sécuritaires auxquels celles-ci doivent répondre.

Réf. PDT-CDC-001	G.I.E. SESAM-VITALE	Page 7 / 24
------------------	---------------------	-------------

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

3.2 Définitions

3.2.1 Réseau local / Réseau distant

On entend par « Réseau local » tout réseau situé dans une zone réduite ou dans un environnement commun, tels qu'un immeuble ou un bloc d'immeubles. Un réseau local devient une partie d'un réseau distant lorsqu'une liaison est établie (via des modems, routeurs distants, lignes téléphoniques, satellites ou une connexion hertzienne) avec un gros système, un réseau de données public (Internet par exemple) ou un autre réseau local.

3.2.2 Exigences sécuritaires

On entend par « exigences sécuritaires » l'ensemble des exigences du GIE SESAM-VITALE en matière de sécurisation des données sensibles et des systèmes traitant ces données.

Ces exigences de sécurité sont de quatre types :

- des exigences générales relatives au respect de la législation française et internationale en vigueur,
- des exigences liées au transport des données sensibles dans le cadre d'un réseau distant,
- des exigences relatives à la sécurité des postes de travail et des équipements des professionnels de santé,
- des exigences relatives à la protection des équipements distants.

En fonction de la configuration, tout ou partie des exigences de sécurité sont applicables.

On distingue parmi ces exigences de sécurité (liste non exhaustive) celles :

- de chiffrement des données : afin de protéger les données sensibles par un mécanisme empêchant qu'un tiers non autorisé y ait accès,
- d'authentification des divers éléments de l'architecture : pour vérifier que tout ou partie des éléments de l'architecture ne soit remplacé par un logiciel malveillant,
- d'intégrité des données et des éléments de l'architecture : pour vérifier que les données et/ou les éléments logiciels de la solution n'ont pas été corrompus,
- ...

Le détail de chacune de ces exigences est fourni dans le présent document.

3.2.3 Analyse sécuritaire

L'analyse sécuritaire d'une solution présentée à l'agrément consiste en une vérification de l'adéquation de celle-ci avec les exigences sécuritaires du GIE SESAM-VITALE.

Page 8 / 24	G.I.E. SESAM-VITALE	Réf. PDT-CDC-001
-------------	---------------------	------------------

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

3.3 L'analyse sécuritaire dans le cadre de la procédure d'agrément

La procédure à suivre pour tout éditeur souhaitant présenter un produit à l'agrément SESAM-Vitale est la suivante :

- lors de la conception de sa solution, l'éditeur doit identifier sur quel type de configuration sa solution se base ;
- en fonction de la configuration adoptée, l'éditeur doit s'assurer que sa solution respecte bien les exigences de sécurité fournies dans le présent document ;
- lors de la signature du protocole d'agrément avec le CNDA, l'éditeur doit déclarer sur quelle configuration ou combinaison de configurations sa solution présentée se base.

Si l'architecture de la solution est conforme à une des configurations « réseau local », aucune analyse sécuritaire n'est nécessaire.

Pour tout autre type d'architecture, un dossier de sécurité doit être transmis au CNDA et au GIE SESAM Vitale. Ce dossier doit présenter de manière analytique la réponse faite aux exigences décrites dans le présent document pour la solution présentée à l'agrément. Ce dossier doit à minima comprendre un schéma de l'architecture de la solution présentée ainsi qu'un tableau réponse fournissant les méthodologies et outils utilisés pour répondre à chacune des exigences de sécurité.

Il est également à noter que le CNDA se réserve le droit de vérifier par toute méthode de son choix la conformité des solutions agréées par rapport aux exigences de sécurité.

3.4 Les architectures « Poste isolé » et « Réseau local »

3.4.1 Généralités

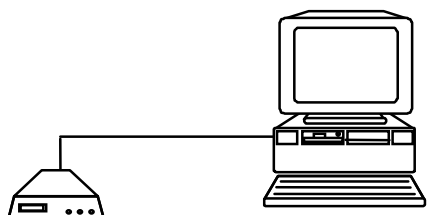
Le présent chapitre décrit les différentes configurations acceptées dans le cadre de l'agrément et qui :

- soit sont constituées d'un poste de travail « isolé » connecté à un ou plusieurs lecteurs,
- soit sont constituées de plusieurs postes de travail fonctionnant dans un « réseau local ».

Dans chacune de ces configurations, les canaux de communication avec les lecteurs de cartes sont ceux pour lesquels ces lecteurs ont été homologués. A cet effet, le Poste de Travail doit obligatoirement disposer d'une connexion disponible compatible avec le lecteur de carte homologué utilisé indépendamment du modem destiné à la connexion vers les réseaux de l'Assurance Maladie ou destiné à toutes autres télétransmission (l'accès au réseau et l'accès à la carte CPS devant s'effectuer simultanément).

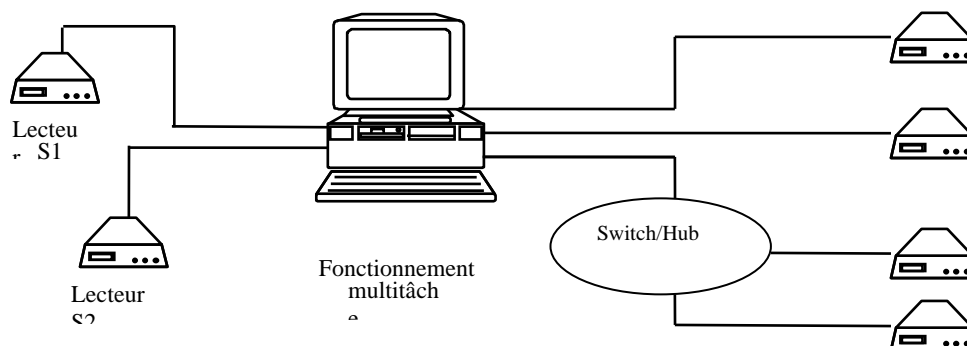
Aucune analyse sécuritaire et technique n'est demandée tant que l'ensemble de la solution reste dans un réseau strictement local (les données sensibles sont confinées dans un espace sous le contrôle du professionnel de santé).

3.4.2 Configuration 1 : Poste de travail mono-canal comportant un lecteur bifente homologué SESAM-Vitale



La liaison entre le poste de travail et le lecteur est obligatoirement une des liaisons pour laquelle le lecteur utilisé a été homologué.

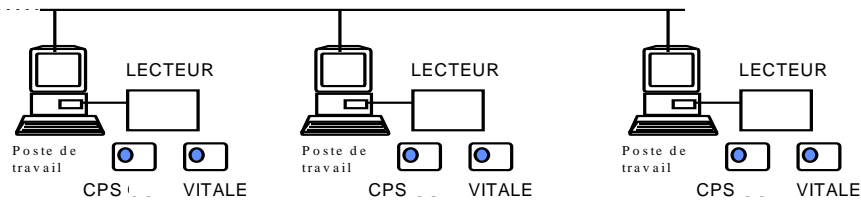
3.4.3 Configuration 2 : Poste de travail avec plusieurs canaux à gérer



On ne peut pas accéder aux lecteurs simultanément.

La liaison entre le poste de travail et le lecteur est obligatoirement une des liaisons pour laquelle le lecteur utilisé a été homologué.

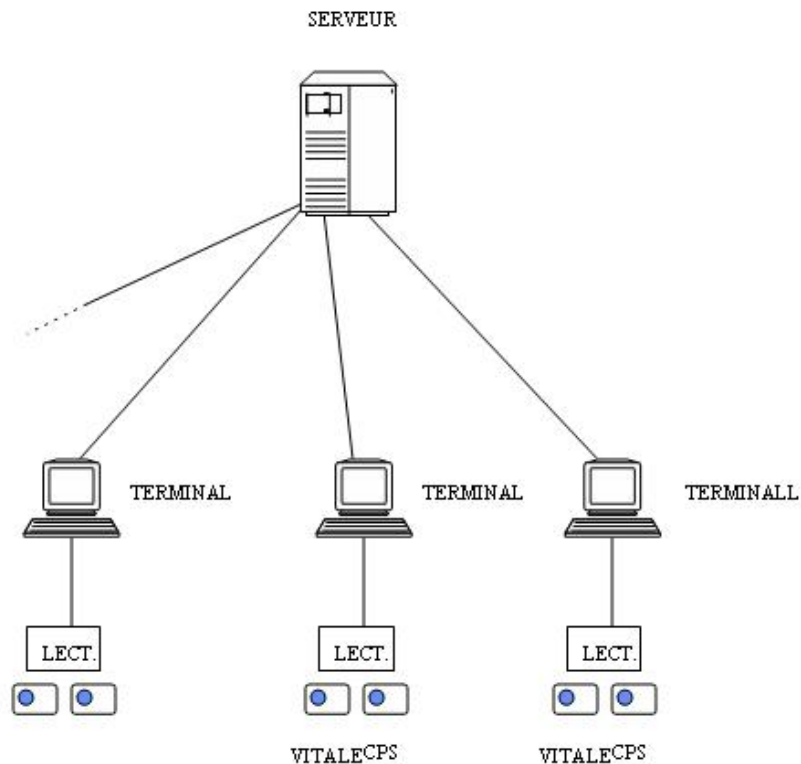
3.4.4 Configuration 3 : Réseau local



Les postes de travail sont connectés les uns aux autres mais restent dans un réseau local.

La liaison entre le poste de travail et le lecteur est obligatoirement une des liaisons pour laquelle le lecteur utilisé a été homologué.

3.4.5 Configuration 4 : Grappe de postes de travail en réseau local



La liaison entre le poste de travail et le lecteur est obligatoirement une des liaisons pour laquelle le lecteur utilisé a été homologué.

Les postes de travail sont connectés à un serveur mais l'ensemble de la solution reste dans un réseau local.

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

3.4.6 Configuration 5 : Configurations « réseau local » mixtes

Chaque poste de travail défini dans la configuration 4 peut être un des postes décrits dans les configurations 1 à 2, indépendamment des autres postes du réseau local.

Les configurations 3 et 4 peuvent être regroupées dans un même réseau local, le serveur de postes de la configuration 4 étant obligatoirement un serveur sur le réseau local. Le serveur de stockage est accessible par les postes de travail réalisant les factures et les lots.

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

3.5 Les exigences sécuritaires

3.5.1 Avant-propos

Ce chapitre a pour objectif de fournir chacune des exigences de sécurité applicables aux solutions présentées dans le cadre de l'agrément sur un réseau distant. Lors de l'élaboration par un tiers d'une solution répondant aux exigences décrites ci-dessous, le GIE SESAM-VITALE s'assurera de la validité des fonctions de sécurité proposées par ce tiers. Le dossier doit impérativement répondre à chacune de ces exigences.

On notera que les exigences de sécurité ne se substituent en aucun cas aux exigences d'autres référentiels tels que, par exemple :

- Décret N°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique,
- décret n°2006-6 du 4 janvier 2006 pour l'agrément des hébergeurs de données de santé à caractère personnel

On notera également que dans le cas où pour quelque raison que ce soit, un éditeur est amené pour sa solution à faire intervenir une société tierce (hébergement d'un serveur...), il reste responsable du respect des exigences de sécurité fournies ici.

3.5.2 Définitions

Termes	Définition
Configuration	La Configuration désigne le système informatique global répondant au cahier des charges SESAM-Vitale
Environnement distant	L'environnement distant désigne un système informatique offrant un service au travers d'une connexion réseau distante.
Réseau	Le réseau désigne l'infrastructure de communication entre un serveur distant et un poste client ou un serveur comportant des nœuds d'interconnexion (PAN, LAN, WAN)
Environnement local	L'environnement local désigne le système informatique situé physiquement dans le local du professionnel de santé.

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

3.5.3 Références externes

Les principaux éléments de la législation française et internationale auxquels le présent chapitre fait référence sont :

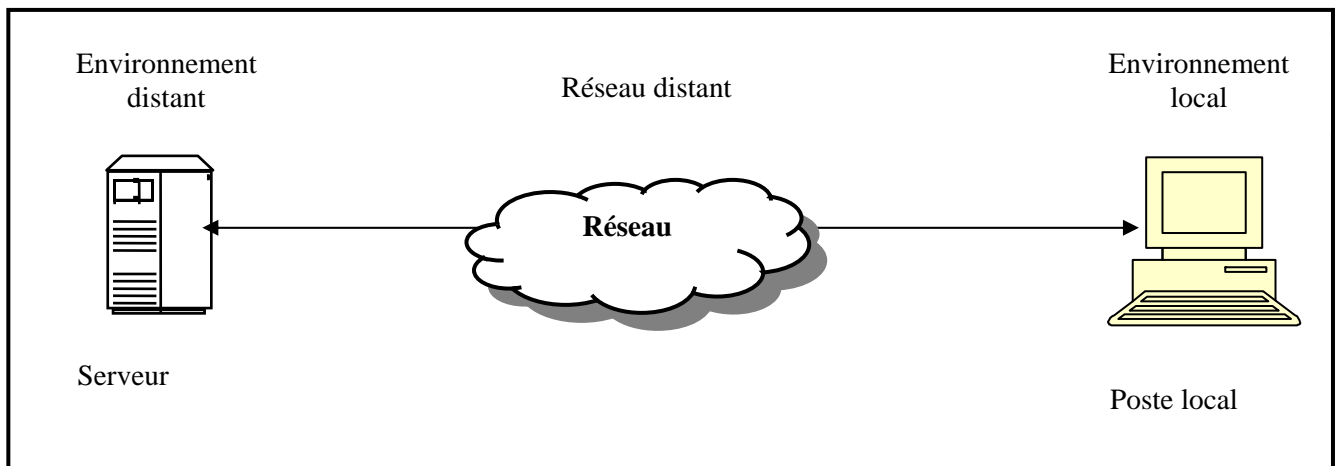
- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) : <http://www.ssi.gouv.fr>
 - o **Mécanismes cryptographiques - Règles et recommandations "standards"**, Rev. 1.10, DCSSI , 12/2006,
 - o **Recommandation n° 901/DISSI/SCSSI** du 2 mars 1994
Recommandations pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense
 - o **Recommandation n° 600/DISSI/SCSSI** de mars 1993
Protection des informations sensibles ne relevant pas du secret de défense
Recommandations pour les postes de travail informatiques
- Commission Informatique et Liberté : <http://www.cnil.fr/>
- Référentiel Générale de sécurité (RGS) v0.98
- The Transport Layer Security (TLS) Protocol Version 1.1: <http://tools.ietf.org/html/rfc4346>
- Ministère de la santé et de la solidarité : Décret n°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique

3.5.4 Architecture des solutions

La solution proposée peut comporter plusieurs sous-systèmes à savoir :

- Un serveur distant (serveur de gestion des équipements, concentrateur de flux, serveur d'application, etc. ...),
- Un poste de travail intégrant un lecteur permettant de lire les cartes Vitale et CPS,
- Un réseau permettant la communication entre les différentes composantes.

D'une manière générale, elle se modélise de la façon suivante :



Les exigences de sécurité sont découpées selon quatre catégories distinctes en fonction de l'élément de l'architecture auxquelles elles s'appliquent. Ces catégories sont les suivantes :

- Exigences générales,
- Exigences liées à l'environnement local,
- Exigences liées à l'échange d'informations via un réseau distant,
- Exigences liées à l'environnement distant.

Les exigences générales s'appliquent à l'ensemble de la solution quelle que soit la configuration adoptée.

Pour chacune des autres catégories le présent document précise à quel niveau de l'architecture elles s'appliquent.

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

3.5.5 Les exigences de sécurité

3.5.5.1 Exigences générales

Informations	Libellé
Confidentialité	La confidentialité, en 2009, doit être assurée par l'utilisation d'un mécanisme de chiffrement avec un algorithme AES – 128 bits ou supérieur . L'algorithme 3DES 112 bits est encore admissible. Le choix de l'algorithme et de la longueur de la clé est susceptible d'évoluer en fonction de l'état de l'art (cf. directives de l'ANSSI entre autres).
Intégrité	L'intégrité, en 2009, doit être assurée par l'utilisation de l'algorithme SHA-256 ou supérieur . L'algorithme SHA-1 est encore recevable pour les composants ne supportant pas encore le SHA-256. Le choix de l'algorithme est susceptible d'évoluer en fonction de l'état de l'art (cf. directives de l'ANSSI entre autres).
Authenticité	L'authenticité, en 2009, doit être assurée par l'utilisation de l'algorithme RSA 1536 bits ou supérieur . L'algorithme RSA 1024 bits est encore admissible. Le choix de l'algorithme est susceptible d'évoluer en fonction de l'état de l'art (cf. directives de l'ANSSI entre autres).
Suite de chiffrement	<p>Dans le cadre du protocole TLS, le GIE SESAM-VITALE recommande l'usage des suites de chiffrement suivantes :</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA</p> <p>Correspondant à l'usage des algorithmes suivants :</p> <p>Echanges de clés : RSA Authentification : RSA Chiffrement : 3DES (112 bits), AES (128 bits), AES (256 bits) Intégrité : SHA-1 / SHA-256</p> <p>Note : En vertu de l'article 30-I de la loi 2004-575 du 21 juin 2004, l'utilisation des moyens de cryptologie est libre.</p> <p>En revanche, la fourniture, l'importation et l'exportation de ces moyens sont réglementées en France. Ces opérations sont soumises soit au régime de la déclaration, soit au régime de l'autorisation. La ANSSI est chargée d'instruire les demandes d'autorisation des moyens et prestations de cryptologie conformément à la législation.</p>

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

3.5.5.2 Exigences pour l'environnement local

Recommandations	Libellé
Réglementation	L'éditeur s'engage à être conforme à la législation française en vigueur (cryptographie, loi informatique et liberté, etc.).
Sensibilisation	Il est recommandé de sensibiliser les utilisateurs à la sécurité du système d'information (par exemple : recommandations dans le manuel utilisateur).
Politique des mots de passe	Les accès aux systèmes d'information doivent être protégés de façon individuelle . Dans le cas d'un usage d'un mot de passe celui-ci doit comporter au moins huit caractères alphanumériques avec des caractères spéciaux. Le mot de passe ne doit pas être un mot du dictionnaire. Il doit être changé de façon régulière, a minima une fois par trimestre et doit être conservé de façon confidentielle.
Correctifs de sécurité	Des mesures doivent inciter l'utilisateur à procéder de façon régulière (hebdomadaire) à la mise à jour de son poste de travail, en particulier pour les mises à jours de sécurités et de l'anti-virus .
Inactivité du système	La session d'un utilisateur ne doit pas être maintenue ouverte au-delà de 60 minutes d'inactivité. Le système doit verrouiller la session automatiquement. La saisie du login/mot de passe est obligatoire pour se reconnecter au système d'information.
Protection virale	Le système d'information doit comporter un système de protection virale pour chaque composant afin de lutter contre l'infection de son propre système et toute propagation sur des systèmes tiers.
Pare-feu	Pour pallier à l'intrusion dans le système d'information via les connexions réseaux, le système doit filtrer les ports et les flux autorisés.
Connexion distante	Toute connexion distante sur le poste local doit être à l'initiative du professionnel de santé. Aucun service distant ne peut accéder au poste local sans l'autorisation du professionnel de santé.
Confidentialité des données	La confidentialité des données stockées dans les bases du progiciel doit être assurée via un chiffrement a minima avec un algorithme AES – 128 bits .
Sauvegarde des données	Des mesures doivent inciter l'utilisateur à procéder de façon régulière à la sauvegarde de ses données et à conserver celles-ci de façon sécurisée dans un autre lieu. La sauvegarde doit être réalisée de façon à garantir l'intégrité et confidentialité des données.
Authentification mutuelle	Les postes clients se connectant à un service distant, doivent authentifier le service auquel ils se connectent. L'utilisation a minima du TLS v1.0 ou TLS v1.1 avec une authentification mutuelle est demandée.
Certificat	L'authentification du poste client est effectuée à partir du certificat de la carte CPS du professionnel de santé. En cas d'atteinte à la confidentialité de la clé (perte ou vol), celle-ci doit faire l'objet d'une demande de révocation auprès de l'autorité émettrice (GIP-CPS).
Vérification d'un certificat	Le certificat présenté par le serveur au poste client doit être valide notamment concernant sa parenté (autorité de confiance), sa validité (date début et de fin) et son usage (authentification serveur).

Réf. PDT-CDC-001	G.I.E. SESAM-VITALE	Page 17 / 24
------------------	---------------------	--------------

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

Liste de révocation	Dans le cadre de l'usage de certificat de confiance, le poste client doit vérifier que le certificat serveur n'est pas révoqué en vérifiant la liste de révocation ou en effectuant une requête OCSP.
Autorité de confiance	L'enregistrement d'une nouvelle autorité de confiance sur le poste client doit faire l'objet d'un consentement du professionnel de santé.
Intégrité des composants	L'intégrité de l'ensemble des composants et des bases de données d'une solution doit être garantie et contrôlée, a minima avec un algorithme SHA-256 ; l'usage du SHA-1 est encore admissible. La corruption de l'un de ces composants doit rendre la solution inutilisable.
Approbation de l'utilisateur	L'utilisateur de la solution doit autoriser explicitement les opérations modifiant le contenu de son progiciel et les tables associées.

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

3.5.5.3 Exigences sur les échanges via un réseau distant

Recommandations	Libellé
Réglementation	L'éditeur s'engage à être conforme à la législation française en vigueur (cryptographie, loi informatique et liberté, etc.).
Connexion	L'établissement d'une connexion doit toujours être à l'initiative de l'utilisateur du poste client.
Négociation des paramètres SSL / TLS	Les paramètres d'une session d'échange SSL / TLS doivent être renégociés toutes les 18 heures.
Chiffrement des données	La confidentialité des données administratives et médicaux-administratives transitant sur tout réseau doit être garantie pendant leur transmission via un chiffrement a minima avec un algorithme AES – 128 bits .
Intégrité des données	L'intégrité des données administratives et médicaux-administratives transitant sur tout réseau doit être garantie pendant leur transmission via l'utilisation à minima de l'algorithme SHA-256 ; l'usage de SHA-1 est encore admissible.

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

3.5.5.4 Exigences pour l'environnement distant

Recommandations	Libellé
Réglementation	L'éditeur s'engage à être conforme à la législation française en vigueur (cryptographie, loi informatique et liberté, etc.).
Infrastructure	Les infrastructures associées au service doivent être dédiées.
Accès au Système	Les accès aux systèmes d'information doivent être protégés de façon individuelle
Politique des mots de passe	Dans le cas d'un usage d'un mot de passe, celui-ci doit comporter au moins huit caractères alphanumériques avec des caractères spéciaux. Le mot de passe ne doit pas être un mot du dictionnaire. Le mot de passe doit être changé de façon régulière, a minima une fois par trimestre et doit être transmis et conservé de façon confidentielle.
Historisation des mots de passe	Dans le cas d'un usage d'un mot de passe, le système distant doit veiller à interdire l'utilisation a minima des trois derniers mots de passe .
Blocage du compte	Le système distant doit mettre en œuvre une mesure afin de se prémunir des tentatives d'accès frauduleux. Il convient de limiter le nombre d'essai à trois dans une même session et de bloquer le compte au bout de dix tentatives infructueuses .
Inactivité d'une session	En cas d'inactivité sur le système d'information, la session d'un utilisateur ne doit pas être maintenue au-delà de 60 minutes en distant. Le système doit soit couper, soit verrouiller la session. Dans le cas d'utilisation d'un login/mot de passe, la saisie de ces derniers est obligatoire pour se reconnecter au système d'information.
Protection virale	Le système d'information doit comporter un système de protection virale sur chaque composant pour lutter contre l'infection de son propre système et la propagation sur les systèmes tiers.
Pare feu	Pour pallier à l'intrusion dans le système d'information via les connexions réseaux, le système doit filtrer les ports et les flux autorisés.
Authentification mutuelle	Lorsque des données sont stockées sur un serveur distant, le service doit identifier et authentifier les équipements ou les utilisateurs qui s'y connectent. L'utilisation a minima du TLS v1.0 ou TLS v1.1 avec une authentification mutuelle est demandée.
Certificat	L'authentification d'un poste client est effectuée à partir d'un certificat émanant de l'autorité du GIP-CPS.
Clé du certificat	La clé du certificat serveur doit être protégée contre les tentatives de lecture illicite. La clé doit être stockée de façon chiffrée. En cas d'atteinte à la confidentialité de la clé (perte ou vol), celle-ci doit faire l'objet d'une demande de révocation auprès de l'autorité émettrice (GIP-CPS).
Liste de révocation	Dans le cadre de l'usage de certificat de confiance, le serveur doit vérifier que le certificat client n'est pas révoqué en vérifiant la liste de révocation ou en effectuant une requête OCSP.
Autorité de confiance	L'enregistrement d'une nouvelle autorité de confiance sur le serveur doit faire l'objet d'une autorisation de l'administrateur.
Chiffrement des	Les données administratives et médico-administratives archivées sur le serveur

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

données	doivent être protégées avec un chiffrement a minima AES – 128 bits .
Intégrité des données	Les données administratives et médico-administratives doivent être stockées sur le serveur de façon intègre.
Intégrité des composants	L'intégrité de l'ensemble des composants logiciels d'une solution doit être garantie et contrôlée. La corruption de l'un de ces composants doit rendre la solution inutilisable.
Etanchéité	Lorsque des données sont stockées sur un serveur distant, celui-ci doit être confiné dans une DMZ dédiée .
Mise à jour de sécurité	Lorsque des données sont stockées sur un serveur distant, ce serveur doit être mis à jour régulièrement pour pallier aux failles de sécurité du système et des applications.
Gestion des habilitations	L'accès au service doit être administré par un système de gestion des habilitations (séparation des rôles). Les rôles de chaque intervenant doivent être clairement identifiés.
Restriction d'accès	Le système distant doit être en mesure suivant l'habilitation de l'utilisateur de restreindre l'accès aux données .
Sauvegarde	Le système distant doit être en mesure d'effectuer une sauvegarde journalière des données. La sauvegarde doit être réalisée de façon à garantir l'intégrité et la confidentialité des données.
Traçabilité	Le système distant doit être en mesure d'historiser les accès à son système d'information et conserver les historiques pendant une période minimale de six mois
Intrusion	Le système distant doit être en mesure d'informer les administrateurs du système en cas de tentative d'intrusion .

3.5.5.5 Note

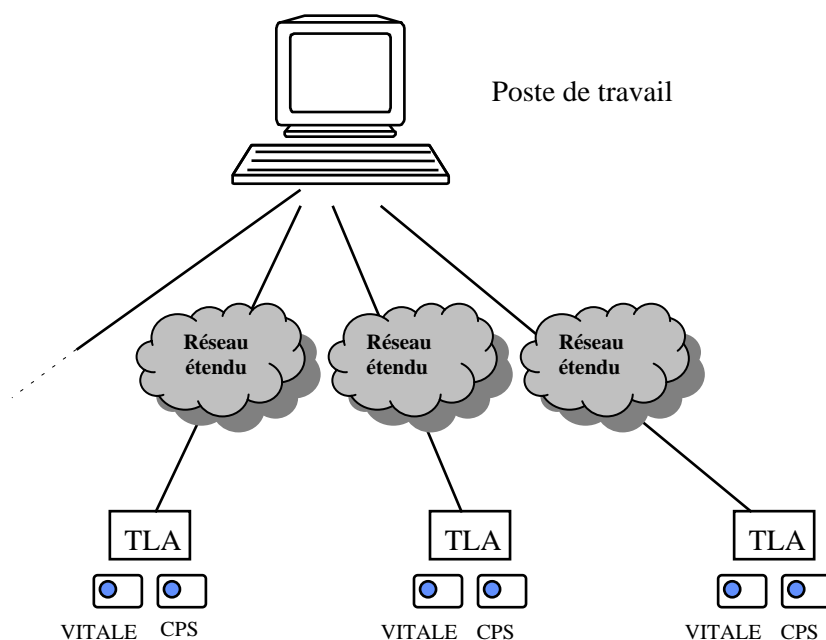
Pour garantir le niveau global de sécurité du système SESAM-Vitale, lors de l'examen de la solution proposée, le GIE SESAM-VITALE peut être amené à compléter ces exigences par des fonctions de sécurité spécifiques adaptées à la solution proposée.

3.6 Les architectures « Réseau distant »

3.6.1 Configuration 6 : TLA(s) distant(s)

Toute configuration proposant la connexion distante entre un TLA et un poste de travail entre dans cette catégorie. Dans cette configuration, le « Poste de travail » peut être soit utilisé dans le cabinet du professionnel de santé soit géré par l'opérateur fournissant la solution de facturation.

NB : Dans cette configuration, seules les fonctionnalités TLA peuvent être utilisés de manière distante.



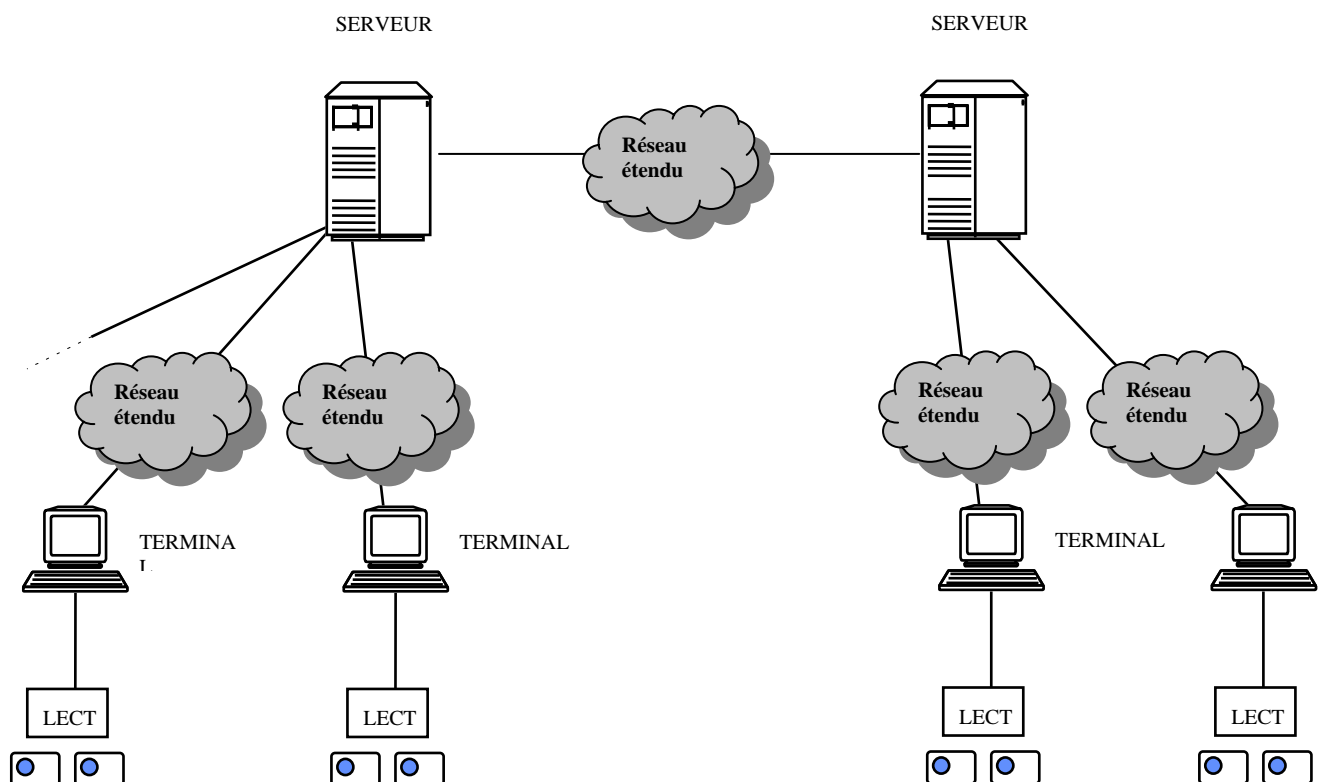
<u>Exigences générales</u>	Ces exigences s'appliquent à l'ensemble de la configuration.
<u>Exigences liées à l'environnement local</u>	Ces exigences s'appliquent à l'ensemble des lecteurs TLA
<u>Exigences liées à l'échange d'informations via un réseau distant</u>	Ces exigences s'appliquent à l'ensemble des connexions entre le poste de travail et les lecteurs TLA
<u>Exigences liées à l'environnement distant</u>	Ces exigences s'appliquent au poste de travail distant.

3.6.2 Configuration 7 : Gestion multiserveurs distants et multi postes de travail distants

Cette configuration décrit la connexion multipostes de travail à de multiples serveurs distants.

Pour cette configuration :

- Le nombre de serveurs est supérieur ou égal à 1,
- des postes de travail peuvent être connectés à un serveur dans un même réseau local,
- deux serveurs au moins peuvent être connectés dans un même réseau local,
- au moins une des connexions « serveur – poste de travail » ou « inter serveurs » opère sur un réseau étendu



Les exigences sécurité applicables sont les suivantes :

<u>Exigences générales</u>	Ces exigences s'appliquent à l'ensemble de la configuration.
<u>Exigences liées à l'environnement local</u>	Ces exigences s'appliquent à l'ensemble des postes de travail
<u>Exigences liées à l'échange d'informations via un réseau distant</u>	Ces exigences s'appliquent à : <ul style="list-style-type: none"> • l'ensemble des connexions distantes entre les postes de travail et les serveurs • l'ensemble des connexions distantes entre les serveurs distants s'il y a plusieurs serveurs.
<u>Exigences liées à l'environnement distant</u>	Ces exigences s'appliquent à l'ensemble des serveurs

NB : Les Progiciels opérant sous CitrixTM ou sous TSETM entrent dans cette configuration.

Annexe 7 version 6.30	Cahier des charges SESAM-Vitale - Ordonnance du 24/04/1996 Version 1.40 – Addendum 6	9 juillet 2010
--------------------------	---	----------------

3.6.3 Configurations 8 : Autres configurations

Cette configuration regroupe toutes les configurations qui ne rentrent dans aucune des configurations de 1 à 7 définies dans le présent document. L'éditeur doit malgré tout déposer au CNDA un dossier sécurité décrivant l'architecture technique et sécuritaire de sa solution. Ce dossier doit être rédigé sur la base des exigences fournies dans le présent document.

<u>Exigences générales</u>	Ces exigences s'appliquent à l'ensemble de la configuration.
<u>Exigences liées à l'environnement local</u>	Ces exigences s'appliquent à l'ensemble des postes de travail
<u>Exigences liées à l'échange d'informations via un réseau distant</u>	Ces exigences s'appliquent à l'ensemble des connexions entre les postes de travail et les serveurs distants ainsi qu'entre les divers serveurs.
<u>Exigences liées à l'environnement distant</u>	Ces exigences s'appliquent à l'ensemble des serveurs